The focus of modern smart card applications, especially in the electronic identity card landscape, has shifted from an approach purely driven by “forgery protection” to a citizen value-centric approach. As such, the creation of user value is key. This article describes the history of and trends relating to smart card applications, mainly focusing on the electronic identity card area.

Introduction
Smart card solutions have seen a broad adoption within the last two decades. Today, billions of smart cards provide easy access to public transportation, are used as secure tokens for payment solutions or protect the card holder’s personal identity in electronic identity documents, and facilitate government services.

History
In the beginning, smart cards were mainly used as secure memories in telephones or in health card applications. Those smart cards were implemented as memory cards without a microprocessor. The e-purse, another high volume application introduced in the 90s, has seen a very broad adoption, especially in Europe, simplifying micro-payments. The global payment industry, represented by Mastercard, VISA and Europay, agreed on the EMVCo standards defining the usage of secure microcontroller-based smart cards in credit/debit card applications. These solutions provide a significantly increased protection against transaction fraud compared to magnetic stripe cards.

SIM cards in mobile phones entered the market in the 90s and have become the leading smart card application with respect to total volume.

In addition, 9/11 triggered a broad adoption of secure smart card solutions in passport and identity card applications to prevent identity theft and to protect countries from illegal immigration and terrorism. At the same time, smart card technology has proved to be a secure and efficient platform for providing citizens access to electronic Government (eGovernment) services, such as social security or healthcare.

Most of the smart card applications listed above have been implemented to protect or simplify models of private businesses (e.g. banking cards) or to support national and international security interests (e.g. electronic passports (ePP), national electronic identity cards (NeID), foreign worker ID cards). The e-purse is one of the few exceptions, providing an increased convenience level to end consumers by enabling cashless micro payments.
Contact and Contactless smart card solutions
The first smart card implementations were contact-based. Contactless smart card solutions were developed mainly by Philips Semiconductors in the early 90s when Philips launched its first Mifare products for a variety of ticketing applications such as ski lifts and mass transit as well as generic building access control applications. Since then, contactless smart cards have been adopted in many applications. However, ticketing, transportation applications and access applications in general are still dominating. Billions of such smart cards have been deployed on a worldwide base. Another high volume contactless security token solution is car immobilizers based on contactless ICs. These devices have helped to decrease the number of car thefts significantly within the last 15 years.

Indeed, contactless smart cards provide a very high convenience level for card holders and high value for issuers. The cards can be read by the reader without physical contact. They can stay in your wallet while the transaction is performed. High transmission rates up to 848kbps can be achieved. Very high bit rate transmission technology is in preparation. As such, transaction times are short and throughput at gates is high. Electronic passports are based on highly secure contactless microcontrollers for smart cards as well.

Contactless solutions also provide clear advantages with respect to reliability, lifetime and durability. Total cost of ownership is much lower compared to contact-based solutions due to lower infrastructure maintenance costs – there is no mechanical abrasion of the reader contacts – and a lifetime of 10 years for a contactless smart card compared to only up to five years for a contact-based smart card.

The German National eID – one of the most sophisticated national eID implementations deployed today – is based on a fully featured contactless smart card IC. The lifetime requirement of 10 years for the eID smart card within this project can only be fulfilled by a contactless solution. Dedicated secure communication protocols secure the contactless data transmission. As such, contactless smart card solutions can be implemented in such ways that the highest security requirements can be met. The same principles apply as for every kind of secure key exchange and secure messaging schemes over open networks. An end-to-end security mechanism needs to be properly applied to realize a highly secure implementation.

The internet created needs which can be perfectly served by secure smart cards
The Internet changed the way we work, communicate, correspond, consume and spend our leisure time. A face to face society has turned into a virtual society. One of the main challenges within such a connected world is to provide instruments that enable users to distinguish between real and faked identities, potential business partners or information. Identification no longer means physical presence – as such, secure identification has turned into secure authentication. Schemes to authenticate and correspond in a legally binding manner are fundamental to capitalising on the opportunities afforded by the most powerful media ever created.

The authenticity of an identity needs to be proven using credentials uniquely connected to a clearly defined entity – which could be a person or any other legal entity – and which can be used solely by this identity. Thus, credentials need to be stored and transmitted secretly. Secure containers able to store secrets and cryptographic communication tools are required to serve those requirements. PC platforms do not comply with those requirements at all, but secure smart card solutions are designed to meet them perfectly. They provide a highly secure platform where confidential data can be stored securely and they come in a portable format ready to be used wherever it is required. As such, they provide real end user value.
There is a fundamental difference between PC platforms and smart cards: smart cards cannot be easily compromised by viruses or Trojan horses, while PC platforms have a high vulnerability with respect to malware. There are many mechanisms implemented that protect secret data on smart cards, and the latest high security smart card solutions – typically used within the applications described in this article – can withstand all known attack schemes without confidential data being disclosed. Independent certification bodies are in place to confirm this level of protection exists before a security certificate for a dedicated smart card application is issued. And because technology evolves on both sides, with attackers getting access to more powerful tools, security technology is also constantly being improved – products are constantly updated to comply with the latest security demands.

**Modern smart card solutions focus on providing user value**

The application focus of modern smart card applications, especially in the electronic identity card landscape, has shifted from an approach purely driven by “forgery protection” to a citizen value-centric approach, as illustrated by Figure 1. This is also true for smart card applications in the payment, access and transportation industry. The creation of user value is key. Contactless smart card solutions are the perfect vehicle for this, as they offer maximum convenience during usage and are compliant with all levels of security requirements.

![Diagram showing the shift in application focus from 2006 to 2012.](image)

- **2006:**
  - eGov applications focused on eMRTDS
  - Int. Travel Security and protection against forgery and fraud
- **2012:**
  - eGov documents address value creation and citizen needs
  - Supporting a connected and IT-determined society
  - eGov applications focused on eMRTDS

**The application focus shifts from a purely forgery protection driven approach to comply to the security interests of nations also to a citizen value centric approach.**

Figure 1: Application focus of smart cards in the electronic identity document area (electronic passport/electronic national identity card) shifts from a purely forgery and fraud protection driven approach to a citizen value centric approach.
Electronic identity cards: Secure Vehicles simplifying our daily life

Beside the need to comply with the highest security requirements, maximization of user value is increasingly dominating the identity card schemes. A major feature of the latest national electronic identity card implementations is that these devices do not just support the physical identification of a person. They are multi-application devices offering additional features that enable card holders to securely navigate through a connected world. Those features, which will be discussed later in this article, provide fundamental user values, as listed in figure 2.

Time and Cost Savings

While online services are widespread, there are still many services which require face to face (F2F) contact, as secure identification is required to provide the service. This is true for many governmental or administrative services such as address change, tax declaration or car registration. It is also true for commercial services such as opening a bank account or applying for insurance. Face to face contact means:

- Time expenditure
- Travel, which is directly related to cost
- Fees to be paid, as there is also a significant cost connected to F2F services on the service provider’s side

ID cards with a secure online authentication function based on strong cryptography provide proven mechanisms to securely identify persons over open networks. Thus, services which can only be provided to securely identified persons can also be offered online. Cost and time advantages are significant on both the citizen and service provider sides – it means fewer kiosks, less staff and faster response times.

Let’s have a closer look at the potential cost savings provided by eGovernment projects in general. It should be recognised that eGovernment projects are still in an emerging state. As such, utilization on the user side is not mature yet due to reasons we will touch on in detail further below.

As of today, there is no comprehensive database available on the realized cost savings based on reliable methods like activity-based costing. One study describes the Impacts of e-government support in least developed countries: a case study of the vehicle registration service in Bhutan: “Using activity-based costing method for internal costs, and assessing quality aspects through staff interviews and customer surveys, significant improvements were found in lead time and adherence to rules felt by citizen users. However, little benefit was found in terms of cost reduction.”

This is typical for eGovernment projects in developing countries with low labor costs and comparably high ICT costs. Cost savings on the staff side are cancelled out by ICT-infrastructure costs. However, the quality, accountability and availability of services in those regions can be increased significantly. This is of high value to citizens in those countries where access to governmental services is not as easy as it is in more developed countries.

---

1 Mayumi Miyata (2011): Measuring impacts of e-government support in least developed countries: a case study of the vehicle registration service in Bhutan, Information Technology for Development, 17:2, 133-152
The picture is quite different in developed countries with high labor costs and comparably low ICT-infrastructure costs. There, the cost saving potential is significant and will materialize with the increased use of eGovernment services. As a result, traditional face to face services can be reduced or even switched off. However, while both service implementations need to be operated in parallel, costs might increase during the transition period.

<table>
<thead>
<tr>
<th>Fundamental citizen/card holder values</th>
<th>Free Elections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost and Convenience Advantages</td>
<td>The fundamental citizen right... to participate in free and independent elections</td>
</tr>
<tr>
<td>Control over identities, data, communication and correspondence</td>
<td></td>
</tr>
<tr>
<td>Time and Cost Savings</td>
<td>Increase of Flexibility</td>
</tr>
</tbody>
</table>

**Figure 2: Fundamental Citizen Values**

**Increased flexibility**
Spatial limitations are no longer a concern if secure authentication schemes enable the provision of online services with strong identification requirements. Time critical tasks can be performed while in the office, abroad on a business trip or on vacation. Citizens need no longer depend on the opening hours of the service provider: internet access is available 24/7.

**Simplification of processes**
Here’s a real world example: the simplification of processes has been the main contributor to the success of health cards introduced in the 90s. With no need to fill in application forms any longer, client management has been significantly simplified, while cost savings and faster response times have also been achieved.

In terms of electronic identity cards offering secure online authentication, processes can be simplified if a person can authenticate reliably based on an official electronic identity. There is no need for a number of security tokens for every special service, each requiring a PIN or password. One official electronic identity can be utilized to access all important online services: administrative/eGovernment services, ebanking, transportation or health/medical services. Secure Single Sign On applications can be easily implemented. As such, one card provides access to a number of important applications, increasing the convenience level and user acceptance significantly.
Other advantages are emerging due to the significantly increased usage of:

- email correspondence
- social networks
- data transfer over open networks
- data storage in open networks

**Control over personal identity and personal data**

Data exchange during an online session might contain a lot of personal data which can be easily spied upon or altered when transmitted over open networks such as the internet. Secure protocol layers such as secure socket layer (SSL), which establish a secure end-to-end messaging channel between the connected parties, can prevent third parties from eavesdropping. However, even when personal data has been provided intentionally by a user over a secured messaging channel, it might be later abused to steal the user’s identity. Secure smart card solutions can provide mechanisms to significantly increase control over personal identities and data. The value of this to the user cannot be overestimated. The damage potential is huge when a personal identity is stolen and abused.

---

2 Smart-Insights Weekly reported in its 2011-37 edition: “The French Interior Ministry claims that there are 80,000 cases of identity theft in France annually”.
3 Javelin Strategy & Research reported in its annual 2011 Identity Fraud Survey Report: “8.1 million people – 3.5 percent of the U.S. population – were victims of identity theft in 2010. That was down 28 percent from 11 million people in 2009. Fraud was down to $37 billion in 2010 from $56 billion in 2009”.

---

There are even mechanisms available that enable card holders to authenticate anonymously and securely without disclosing any personal data. This can be a requirement of card holders when entering chat rooms or platforms where they prefer to stay anonymous. As such, privacy concerns can also be fully addressed. Citizen-friendly implementations of electronic identity solutions complying with data privacy protection requirements are possible, which means that “Big Brother” doesn’t have to be around every corner.

Another feature and a very good example of minimizing the disclosure of personal data is the “age verification” feature. Many online services require age verification, typically connected to disclosure of all personal data (name, address, birth date etc). An age verification function on the ID card is able to simply confirm whether a card holder meets the minimum age requirement without disclosing any further personal data. Additionally, children can be reliably excluded from accessing restricted services.
**Ability to prove authenticity of identities plus authenticity and integrity of data:**
The ability to prove the authenticity of identities such as potential business partners or chat partners, plus the ability to ensure the authenticity and integrity of data (e.g. when performing financial transactions) are vital in an increasingly virtual world. “What you see is what I am” or “what you see is what you get” is no longer always the case. Web pages with fake identities have flooded the internet and are a real threat – just think of the many incidents of vulnerable youngsters being misled by predatory adults hiding behind false identities in chat rooms; or the huge number of phishing attacks, where criminals attempt to obtain PINs or TANs to access to bank accounts. The damage due to phishing attacks has been roughly 17M Euro in Germany in 2010 according to the Bitkom and German Bundeskriminalamt.

Secure smart card solutions support mechanisms allowing both parties connected via an open network to securely and reliably identify each other via a mutual authentication scheme. In parallel, a secure messaging channel is established to protect the connection from eavesdropping. Based on such solutions, trust can be established between the partners. Personal and confidential data can be exchanged while the authenticity and integrity of identities and data can also be assured.

The German National eID (neuer deutscher Personalausweis) implementation is strongly focusing on satisfying the needs described above. This eGovernment document comes with online authentication functionality where privacy, data minimization and data self-determination requirements have been fully considered. Before any personal data is sent by the smart card during an online authentication procedure, the card holder needs to approve whether he is willing to provide any personal data and if yes, what subset of data, stored on the card, he is willing to disclose. A mutual authentication protocol ensures whether the server/terminal the user is connected to is based on an officially approved identity and has the correct access rights to the personal data stored on the identity card.

Such a scheme can be realized based on smart card verifiable certificates that the server needs to provide during the mutual authentication procedure. The smart card is able to verify whether the certificate is valid and has been issued by an official certification authority. As such, the cardholder can be sure that the authenticity of the service provider – which could be an online shop – has been officially validated and approved. The effort to install and maintain a system able to provide such functionality is significant. A complex multi-level public key infrastructure needs to be in place.

---

4 Bitkom, September 6th 2010: Online-Kriminelle gehen immer raffinierter vor
**Legal Certainty**

Since it is comparably simple to falsify and alter data sent over open networks, standard email correspondence, which is typically sent in unencrypted form, does not provide legal certainty. Dedicated schemes are required to ensure the authenticity and integrity of online correspondence before legal certainty can be acknowledged. Since online correspondence has become standard within business to business, business to consumer and especially consumer to business communication, citizens need access to a mechanism which allows them to electronically send legally binding documents.

A qualified electronic signature (QES) solution, which is typically implemented in modern national electronic identity documents, provides this kind of mechanism. It allows citizens to electronically sign documents in a legally binding manner. Also here a public key infrastructure needs to be in place to support the scheme. The digital signature ensures the integrity of the document and binds it in a unique way to the citizen. It can only be performed by the cardholder using a password to provide access to the qualified electronic signature application on the smart card.

This powerful and sensitive application requires the cardholder to be fully aware of how to use it and the risks connected to it, as there is a significant damage potential. Misuse needs to be avoided under all circumstances. As such cardholders need to be properly educated. The implementation of a QES should be based on state of the art smart card technology complying with the highest security requirements. For this kind of application, special smart card readers – so called Class 2 smart card readers with integrated keypad – are highly recommended to protect the password from eavesdropping. With proper handling and equipment, the QES function provides a powerful and reliable tool.

**THE fundamental citizen right: Participation in free elections – the e-voting card**

The smart card functionalities described above can be leveraged in countries that have a powerful ICT infrastructure in place. This is mainly true for developed countries. But as pointed out earlier in this article, smart card projects in developing countries can have a completely different focus. Having access to governmental services is not always a given in such regions. As such, eID multi-application smart card solutions might combine social security card, health card and e-voting card functionality, providing access to fundamental services and supporting fundamental citizen rights.

The Indonesian eKTP project is one of the largest national eID projects currently in rollout. It also relies on a contactless solution. Deployment started in late 2011, and roughly 170 million citizens out of 240 million will receive an eID card. One main requirement of this solution is to provide an e-voting function beside the eID function. As such, the eKTP ID project provides strong user value by supporting a fundamental right of citizens within a democratic society.
Obstacles and mindset issues to be overcome

Several large scale projects in the electronic identity card area have been deployed within the last decade, providing online authentication, digital signature, governmental services or e-voting features. As already mentioned earlier, one of the implementations considering user value in a very sophisticated manner and currently in deployment is the German National eID. Many more projects are in preparation worldwide.

User Acceptance of eID solutions is directly connected to Value Add brought to users

- System implementations need to consider Ease of Use
- Properly explained and transparent use schemes based on secure implementations create trust

Figure 3: Pre-requisites to achieve user acceptance
However, if we look at the numbers of activated and heavily utilized smart cards in the identity card area providing features such as online authentication and qualified electronic signature capability, user acceptance of such solutions is not yet at the expected level due to the pre-requisites described in figure 3.

**User Value:**

1. Value adds and opportunities connected to usage are not really understood by users. Users need to be informed and educated much better on the capabilities of such solutions.

**Ease of Use:**

2. There is currently no adequate installed reader base at home. Secure Class II readers need to be made available for a reasonable price.

3. Middleware solutions are not user-friendly. User-friendly implementations need to be developed and seamlessly integrated in IT solutions.

**Trust:**

4. Risks are perceived to be high (e.g. in case of misuse of the digital signature, liability is with the cardholder). Users need to be informed and educated. Legislation might need to be adapted to properly distribute risks.

5. People are expecting “big brother” behind such kind of solutions. Also here, open user information is required to create trust.

Deployment of electronic identity cards needs to be accompanied by an open and transparent discussion on opportunities and risks. Easy to understand guidelines on how to use features properly need to be provided. Adequate and low priced reader equipment (class 2 readers with keypad to allow secure PIN/PWD entry), user friendly middleware solutions and a high adoption rate on the service provider side are required to achieve broad user acceptance. Ultimately, trust in the solution and ease of use combined with maximized user value are determining whether cardholders will really use these high security tokens in their daily lives.

Finally, a high utilization rate on the user side is a basic prerequisite for proper return on investment. User acceptance and utilization rates will determine whether potential cost savings materialize, especially within eGovernment projects.
**Trends and Future Outlook**

A modern society which increasingly relies on online services requires technology that can provide a “personal secure identity”. It is a fundamental prerequisite for an open and secure ICT-connected society where commercial and public businesses and services can prosper. Smart card technology has proven over time to be an adequate platform to host such a personal identity.

In developed countries, almost everybody carries secure microcontroller-based smart cards or security tokens in their pockets. Beside the electronic identity cards described in this article, smart card schemes providing payment, micro purse and transportation functionality within a multi-application set-up have gained highest user acceptance.

They provide real user value and a high level of convenience. This kind of smart card solution has been mainly deployed by banks or citizen card companies in a regional context. Further features are expected to be added to those schemes in the future, also covering electronic identity features.

Latest secure microcontroller developments are simplifying the development and deployment of these multi-application solutions, providing hardware platforms optimized for the secure operation of several applications on one device. As there is a clear trend toward contactless smart card solutions, there is also a clear trend towards multi-application.

National eID cards will be deployed in large volume on a worldwide basis within the next few years. Some of them will focus on providing features supporting citizens to securely identify themselves in offline and online situations as well as providing qualified digital signature functionality. Others will also implement commercial applications beside the “personal identity” functionality controlled by government authorities. However, the installed reader base in homes is still small and therefore utilization rates are not as high as expected.

Adoption is expected to increase in the coming years with the introduction of NFC in mobile phones, personal computers and tablet PCs as standard feature. This will overcome the at-home-infrastructure issue. Class II readers could be easily implemented.

With the exponential growth of transactions over the internet, secure authentication schemes are getting more and more important. Most of the current IT-based solutions do not provide a satisfying security level. This is very much related to the vulnerability of PC-platforms in general. Authentication schemes implemented in national eID cards comply with the latest security requirements and offer a much more secure solution which could be easily utilized by banks to secure payment transactions over the internet.

There is also a strong trend towards mobile platforms. Smart phones are powerful “always on” platforms providing access to the full range of online services. As such, integrated secure microcontrollers, called secure elements, can provide the same functionality as smart cards do. However, national electronic identity documents in the ID-1 card format with implemented physical security features are expected to stick to this form factor since the main purpose is still secure identification for national authorities. Considering problems relating to battery life, smart phones are seen more as a back-up solution to carrying a copy of your ID or electronic driver’s license. We expect a clear separation of those applications mainly driven by official authorities, while commercial applications are free to migrate to platforms where the benefits on the user and service provider sides can be maximized.